

What Is Claimed Is:

Sub A37

1 1. A method for sharing a secure communication session with a client
2 between a plurality of servers, comprising:
3 receiving a message from the client at a first server in the plurality of
4 servers, the message including a session identifier that identifies a secure
5 communication session with the client; and
6 if the session identifier does not correspond to an active secure
7 communication session on the first server, establishing an active secure
8 communication session with the client on the first server by,
9 attempting to retrieve state information associated with the
10 session identifier for an active secure communication session
11 between the client and a second server from the plurality of
12 servers,
13 if the state information for the active secure communication
14 session is retrieved, using the state information to establish the
15 active secure communication session with the client without
16 having to communicate with the client, and
17 if the state information for the active secure communication
18 session is not retrieved, communicating with the client to establish
19 the active secure communication session with the client.

1 2. The method of claim 1, wherein attempting to retrieve the state
2 information includes:
3 attempting to use the session identifier to identify the second server in the
4 plurality of servers that has an active secure communication session with the
5 client that corresponds to the session identifier; and

Sub A³ 7

6 attempting to retrieve the state information from the second server.

1 3. The method of claim 1, wherein attempting to retrieve the state
2 information involves attempting to retrieve the state information from a
3 centralized repository that is in communication with the plurality of servers.

1 4. The method of claim 3, wherein the centralized repository includes
2 a database for storing the state information.

1 5. The method of claim 1, wherein establishing the active secure
2 communication session involves establishing a secure sockets layer (SSL)
3 connection with the client.

1 6. The method of claim 1, wherein the state information includes:
2 a session encryption key for the secure communication session;
3 the session identifier for the secure communication session; and
4 a running message digest for the secure communication session.

1 7. The method of claim 6, further comprising:
2 using the message to update the running message digest; and
3 checkpointing the updated running message digest to a location outside of
4 the first server.

1 8. The method of claim 1, further comprising, if the state information
2 for the active secure communication session is retrieved, purging the state
3 information from a location from which the state information was retrieved, so

Sub A37

4 that the state information cannot be subsequently retrieved by another server in the
5 plurality of servers.

1 9. The method of claim 1, further comprising initially establishing an
2 active secure communication session between the client and the second server, the
3 active secure communication session being identified by the session identifier.

1 10. The method of claim 1, wherein attempting to retrieve the state
2 information includes authenticating and authorizing the first server.

1 11. A method for sharing a secure communication session between a
2 plurality of servers, comprising:
3 sending a message from a client to a first server in the plurality of servers,
4 the first server having no active secure communication session with the client, the
5 message including a session identifier;
6 receiving a response to the message from the first server; and
7 if the response indicates that no active secure communication session has
8 been created with the client on the first server, communicating with the first server
9 to establish an active secure communication session.

1 12. The method of claim 11, wherein the client sends the message to
2 the first server only if an active secure communication session is held by a second
3 server in the plurality of servers, wherein the second server has an address that is
4 related to the address of the first server.

1 13. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform a method for sharing

Sub A³ 7

3 a secure communication session with a client between a plurality of servers, the
4 method comprising:
5 receiving a message from the client at a first server in the plurality of
6 servers, the message including a session identifier that identifies a secure
7 communication session with the client; and
8 if the session identifier does not correspond to an active secure
9 communication session on the first server, establishing an active secure
10 communication session with the client on the first server by,
11 attempting to retrieve state information associated with the
12 session identifier for an active secure communication session
13 between the client and a second server from the plurality of
14 servers,
15 if the state information for the active secure communication
16 session is retrieved, using the state information to establish the
17 active secure communication session with the client without
18 having to communicate with the client, and
19 if the state information for the active secure communication
20 session is not retrieved, communicating with the client to establish
21 the active secure communication session with the client.

1 14. The computer-readable storage medium of claim 13, wherein
2 attempting to retrieve the state information includes:
3 attempting to use the session identifier to identify the second server in the
4 plurality of servers that has an active secure communication session with the
5 client that corresponds to the session identifier; and
6 attempting to retrieve the state information from the second server.

Sub A³ 7

1 15. The computer-readable storage medium of claim 13, wherein
2 attempting to retrieve the state information involves attempting to retrieve the
3 state information from a centralized repository that is in communication with the
4 plurality of servers.

1 16. The computer-readable storage medium of claim 15, wherein the
2 centralized repository includes a database for storing the state information.

1 17. The computer-readable storage medium of claim 13, wherein
2 establishing the active secure communication session involves establishing a
3 secure sockets layer (SSL) connection with the client.

1 18. The computer-readable storage medium of claim 13, wherein the
2 state information includes:
3 a session encryption key for the secure communication session;
4 the session identifier for the secure communication session; and
5 a running message digest for the secure communication session.

1 19. The computer-readable storage medium of claim 18, wherein the
2 method further comprises:
3 using the message to update the running message digest; and
4 checkpointing the updated running message digest to a location outside of
5 the first server.

1 20. The computer-readable storage medium of claim 13, wherein the
2 method further comprises, if the state information for the active secure
3 communication session is retrieved, purging the state information from a location

Sub A³7

4 from which the state information was retrieved, so that the state information
5 cannot be subsequently retrieved by another server in the plurality of servers.

1 21. The computer-readable storage medium of claim 13, wherein the
2 method further comprises initially establishing an active secure communication
3 session between the client and the second server, the active secure communication
4 session being identified by the session identifier.

1 22. The computer-readable storage medium of claim 13, wherein
2 attempting to retrieve the state information includes authenticating and
3 authorizing the first server.

1 23. A computer-readable storage medium storing instructions that
2 when executed by a computer cause the computer to perform a method for sharing
3 a secure communication session between a plurality of servers, comprising:
4 sending a message from a client to a first server in the plurality of servers,
5 the first server having no active secure communication session with the client, the
6 message including a session identifier;
7 receiving a response to the message from the first server; and
8 if the response indicates that no active secure communication session has
9 been created with the client on the first server, communicating with the first server
10 to establish an active secure communication session.

1 24. The computer-readable storage medium of claim 23, wherein the
2 client sends the message to the first server only if an active secure communication
3 session is held by a second server in the plurality of servers, wherein the second
4 server has an address that is related to the address of the first server.

Sub A³ 7

1 25. An apparatus that shares a secure communication session with a
2 client between a plurality of servers, comprising:
3 a receiving mechanism, at a first server in the plurality of servers, that
4 receives a message from the client, the message including a session identifier that
5 identifies a secure communication session with the client;
6 an examination mechanism that examines the session identifier; and
7 a session initialization mechanism, on the first server, wherein if the
8 session identifier does not correspond to an active secure communication session
9 on the first server, the session initialization mechanism is configured to establish
10 an active secure communication session with the client by,
11 attempting to retrieve state information associated with the
12 session identifier for an active secure communication session
13 between the client and a second server from the plurality of
14 servers,
15 if the state information for the active secure communication
16 session is retrieved, using the state information to establish the
17 active secure communication session with the client without
18 having to communicate with the client, and
19 if the state information for the active secure communication
20 session is not retrieved, communicating with the client to establish
21 the active secure communication session with the client.

1 26. The apparatus of claim 25, wherein the session initialization
2 mechanism is configured to attempt to retrieve the state information by:

Sub A37

3 attempting to use the session identifier to identify the second server in the
4 plurality of servers that has an active secure communication session with the
5 client that corresponds to the session identifier; and
6 attempting to retrieve the state information from the second server.

1 27. The apparatus of claim 25, wherein the session initialization
2 mechanism is configured to attempt to retrieve the state information by attempting
3 to retrieve the state information from a centralized repository that is in
4 communication with the plurality of servers.

1 28. The apparatus of claim 27, wherein the centralized repository
2 includes a database for storing the state information.

1 29. The apparatus of claim 25, wherein the active secure
2 communication session includes a secure sockets layer (SSL) connection with the
3 client.

1 30. The apparatus of claim 25, wherein the state information includes:
2 a session encryption key for the secure communication session;
3 the session identifier for the secure communication session; and
4 a running message digest for the secure communication session.

1 31. The apparatus of claim 30, further comprising an updating
2 mechanism that is configured to:
3 use the message to update the running message digest; and to
4 checkpoint the updated running message digest to a location outside of the
5 first server.

Sub A³7

1 32. The apparatus of claim 25, further comprising a purging
2 mechanism that is configured to purge the state information from a location from
3 which the state information was retrieved, so that the state information cannot be
4 subsequently retrieved by another server in the plurality of servers.

1 33. The apparatus of claim 25, wherein the session initialization
2 mechanism is configured to authenticate and authorize the first server prior to
3 receiving the state information.

1 34. An apparatus that facilitates sharing a secure communication
2 session between a plurality of servers, comprising:
3 a sending mechanism that sends a message from a client to a first server in
4 the plurality of servers, the first server having no active secure communication
5 session with the client, the message including a session identifier;
6 a receiving mechanism that receives a response to the message from the
7 first server; and
8 a session initialization mechanism that communicates with the first server
9 to establish an active secure communication session with the first server if the
10 response indicates that no active secure communication session has been created
11 with the client on the first server.

1 35. The apparatus of claim 34, wherein the sending mechanism sends
2 the message to the first server only if an active secure communication session is
3 held by a second server in the plurality of servers, wherein the second server has
4 an address that is related to the address of the first server.